CYBER CRIME

Ileana ŞTEFAN*

ABSTRACT: *Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.*

KEYWORDS: *cyber crime, criminal activities, cyberspace, illegal action, IT systems*
JEL CLASSIFICATION: *K 00, K 14*

The use of the web presents a series of advantages and disadvantages. One of the disadvantages is cyber crime, formed of illegal activities committed through the internet.

Cyber crime is a criminal activity in which the object of the crime is the use of the computer and of the net.

This phenomenon is defined differently by the professionals of the field, without a unanimously accepted definition, due to the complexity of this criminal act, and the different regulations from individual states led to the impossibility of the development of an international pattern.

One of the definitions defines the act as "any illegal action in which a computer is the instrument or the object of the crime, any crime that has as means or aim influencing the operation of a computer."(1)

The expert group within the OECD adopted a working definition on the topic: "informational abuse is any illegal conduct or contrary to ethics or unauthorized that regards an automatic treatment of data and/or transmission of data."

Cyber crime can be defined as being the crimes against IT systems, that compromise all crimes that can be committed through internet and IT systems.

Another definition is based on the computerization and on the existence of computer networks. These systems allow the administration of data bases and allow financial operations through electronic payment methods. Moreover, it can be observed that computers and the internet are more often used for committing common offences (prostitution, pimping, child pornography, forgery, blackmail, etc.)

* Lecturer, PhD., "Petru Maior" University of Tg. Mureş, Faculty of Economics, Law and Administrative Sciences, ROMANIA.

Cyber crime includes everything, from illegal download of music files to the stealing of millions of EURO from bank accounts. Cyber crime also includes nonmonetary crimes such as the creation and distribution of viruses from other computers and the posting of confidential business information.

One of the most common forms of cyber crime is the theft of identity, in which the internet is used by criminals to steal personal information from other users. Users are encouraged to use sites that appear to be legitimate but in reality they are fake, asking for personal information, such as login information, composed of the introduction of the user name and password, phone numbers, credit card numbers, bank account numbers. Thus, this information can be used by criminals to steal the "identity" of another person. This is the reason why precautionary measures such as the verification of the URL or of the site address are recommended in order to ensure the protection of your personal information.

Because the cyber crime phenomenon regards a large sphere of criminal activities, the above examples are just one of the thousands of crimes that are taken into consideration in the virtual space. Even if the use of computers and of the internet network have benefic effects, it is unfortunate that some people use these technologies to take advantage of others.

It is recommended to make a distinction between the inappropriate use of an IT system and a fraud or between the use without knowledge about effect of computer keys and the unauthorized use of a network. The use of a password by a user, even he or she received the password from another user, cannot be considered a crime. On the other hand, if the password was stolen and used, this can be considered a cyber crime.

In an article in National Research Concelia "Computers at Risk", Nandini Ramprasad says:

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

Mr. Pavan Duggal, who is the President of cyberlaws.net and consultant, in a report has clearly defined the various categories and types of cybercrimes.

Cybercrimes can be basically divided into 3 major categories:

1. Cybercrimes against persons.
2. Cybercrimes against property.
3. Cybercrimes against government.

Cyber crimes committed against persons consist of activities as: the posting of obscene and/or xenophobe materials, of pornographic materials (especially those regarding children), racist materials or those that instigate to violence, harassment of any nature (sexual, racial, religious) by the use of computers (for example by mail), the violation of private life (collection, storage, modification and disclosure of personal data)

Cyber crimes committed against persons include the following types of actions:

- Access of unauthorized data, as well as the disclosure and spread of these data (even if it is not personal data);
- Change, forgery and use of data with the intent to produce damage;
- Collection, storage and recording of data that is not public;
- Keeping data bases that do not correspond with the reality.

One example of such crime that produced a big damage not only to one person but to a great mass of people was the virus called Melissa. This virus appeared on the net in 1999 and harmed IT networks in Europe and the USA, causing damage estimated to 80 million dollars.

In the USA the virus infected 1,200,000 computers, affecting one fifth of the big companies in the country.

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful software.

The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

The main *elements* that determined the reorientation of criminal groups towards cyber crimes (Juridice.ro):

- Great profit within a relatively short time and with minimal risks;
- the trans-border nature of the crimes, because in order to prove the act in many cases information from many states is necessary, through international legal cooperation means, the procedure being costly and slow;
- The easy access to modern equipment that allow complex illicit activities;
- the possibility for group members to move from one state to another, and the tracking of these activities being, in many cases very difficult by national authorities.

Crimes defined by the Cyber Crime Convention are presented in what follows (criminalitate.info):

1. Illegal access to an IT system, defined by article 2 of the Convention, illegal access is incriminated in order to protect the integrity of these systems without reference to the type of the attack that is used. The crime of accessing with no right the computer system is stipulated in the art. 42 of the Computer Crime Law. The text stipulates as it follows:

"(1) The access, without right, of the computer system constitutes a crimes and it is punished with jail from 6 months to 3 years or with fine.

(2) If the deed stipulated in the paragraph (1) is undergone by breaking the security measures, the punishment is from 3 to 12 years."

The legal regulation is meant to protect the computer information systems and the saved data on these by the unauthorised access to them.

2. Illegal interception of non-public transmissions, defined by article 3 of the Convention and has as purpose to protect communications and transmitted data with the help of an IT system, interception realized without having the right and with the use of technical means. It is to be observed that this interception has to be committed with intent and the article allows states to request intent as a condition for incrimination. The crime of intercepting, without the right, of a computer information data transmission that is not

public is stipulated in the art. 43 of the Computer Crime Law. The text of the law stipulates as it follows:

"(1) Intercepting, without the right, a computer data transmission that is not public and that is destined to a computer information system, that comes from such a system or is undergone within a computer system, constitutes a crime and is punished with jail from 2 to 7 years.

(2) With the same punishment there is sanctioned also the interception, without right, of an electromagnetic emission originated in a computer information system that contains computer data that are not public."

3. Interference with computer data. Interference on data from an IT system realized by the deletion, damage and change of data, committed with intent is defined by article 4 of the Convention, allows states to determine the condition that the damage is required to be with grave consequences. This legal norm defends the integrity of computer data. This norm defends the integrity of the computer data. The crime is regulated by the art. 44 of the Computer Crime Law, the text mentioning:

"(1) The deed of modifying, deleting or deteriorating computer data or restricting the access to these data, without right, constitutes a crime and it is punished with jail from 2 to 7 years.

(2) The unauthorised data transfer from a computer information system is punished with jail from 3 to 12 years.

(3) With the punishment stipulated at paragraph (2) there is sanctioned also the unauthorised data transfer from a computer data saving device."

4. Interference with IT systems. The protection of IT systems is regulated by article 5 of the Convention, article that incriminates the damage on the normal functioning of IT systems through different means such as the introduction of data, the damaging, deletion, alteration or blocking of data. This is a norm meant to protect the good functioning of computer infrastructure that represents the keys of many domains as well as of telecommunications. The crime, stipulated in the art. 45 of the Computer Crime Law, is regulated by the following text:

"The deed of seriously disturbing, with no right, the functioning of a computer information system, by introducing, transmitting, modifying, deleting or deteriorating computer data or by restricting the access to these data constitutes a crime and it is punished with jail from 3 to 15 years."

5. The use of computer technology for illegal purposes. Being provided by article 6 of the Convention, the illegal use is defined by the paragraphs of the article:

· Production, sale, procurement, distribution of technology (including software) designated to allow the perpetration of crimes.

· Production, sale, procurement, distribution of passwords and access keys by which one can access IT systems with criminal intent

· The possession of the above mentioned technologies for criminal ends.

The Convention underlines that the acts are incriminated only if there are committed with intent. The crime, stipulated in the art. 45 of the Computer Crime Law, is regulated by the following text:

"(1) There constitutes a crime and it is punished with jail from 1 to 6 years:

a) the deed of producing, selling, importing, distributing or making available, under any other form, with no right, a computer device or program conceived or adapted in order to commit one of the crimes stipulated in the art. 42-45;

b)) the deed of producing, selling, importing, distributing or making available, under any other form, with no right, an access password, code or any other similar computer data that allow the total or partial access to a computer information system in order to commit one of the crimes stipulated in the art. 42-45.

(2) With the same punishment there is sanctioned also owning, with no right, a device, a computer program, a password, an access code or computer data from those stipulated in the paragraph (1 in order to commit one of the crimes stipulated in the art. 42-45."

6. Forgery of computer data. According to article 7 of the Convention, forgery by alternation, deletion, blocking, etc. of data within an IT system has to be incriminated. This norm defends the integrity of data with legal value.

The crime is stipulated in the 48 of the Computer Crime Law. The law text stipulates:

"The deed of introducing, modifying or deleting, with no right, computer data or restricting, with no right the access to these data, resulting in data that are accordingly to the truth, in order to be used for committing a legal consequence, constitutes a crime and it is punished with jail from 2 to 7 years".

7. The fraudulent use of IT systems. According to article 8 of the Convention, the alteration of data as well as the interference with the functioning of an IT system for criminal ends is incriminated.

The crime is stipulated in the art. 49 from the Computer Crime Law. The text stipulates:

"The deed of causing a patrimonial prejudice to a person by introducing, modifying or deleting computer data, by restricting the access to these data or by preventing in any way the functioning of a computer information system, in order to get a material benefit for yourself or for others, constitutes a crime and it is punished with jail from 3 to 12 years."

8. Child pornography. Incriminated by article 9 of the Convention, it is largely defined in order to include the various forms of manifestations of these crimes, including the possession of pornographic materials with children – all of these crimes being related to IT systems. The crime is stipulated in the art. 51 of the Computer Crime Law. The text stipulates:

"(1) There constitutes a crime and it is punished with jail from 3 to 12 years and interdiction of some rights, producing for sharing, offering or making available, sharing or transmitting, getting for yourself or for others, pornographic materials with under-aged children by using computer information systems, or owning, with no right, pornographic materials with under-aged children by a computer information system or by a computer data saving device.

(2) The attempt is punished."

9. Protection of copyright. Article 10 of the Convention has the role to harmonize the efforts of incrimination of copyright violations in the member states. The crime of allowing, with no right, the public access to the computer data bases that contain or

constitute protected works is stipulated in the art. 140, let. c of the Law no. 8/1996, referring to the copyright and related rights.

The law text stipulates:

"There constitutes a crime and it is punished with jail from one month to 2 years or fine from 200.000 lei to 3 million lei, if it doesn't constitute a more serious crime, the deed of the person that, without having the authorisation or, according to the case, the consent of the copyright owner recognised by the hereby law:

...

c) it allows the access to public computer data bases, that contain or constitute protected works."

REFERENCES

Maxim Dobrinoiu – "Infractiuni in domeniul informatic", Ed. C.H. Beck , Bucuresti 2006
I. Vasiu, *Drept şi Informatică. Protecţia juridică a programelor*, Studii de drept românesc, Ed. Academiei Române, 1993
I. Vasiu, L. Vasiu, *Informatica Juridică şi Drept Informatic*, Ed. Albastră, 2002
T. Amza, C.P. Amza, *Criminalitatea Informatică*, Ed. Lumina Lex, 2003
I. Vasiu, *Criminalitatea Informatică*, Ed. Nemira, 1998
D. Oprea, *Protecţia si Securitatea Informaţiilor*, Ed. Polirom, 2003
Legea nr. 161/2003
Legea nr. 8/1996
http://www. Juridice.ro
http://www.criminalitate.info